

**Prepared Statement of  
The Federal Trade Commission**

**Before the**

**Committee on Energy and Commerce  
Subcommittee on Commerce, Trade, and Consumer Protection  
United States House of Representatives**

**Hearing on Online Pornography:  
Closing the Door on Pervasive Smut**

**Washington, D.C.**

**May 6, 2004**

Mr. Chairman and members of the Committee, I am Howard Beales, Director of the Bureau of Consumer Protection, Federal Trade Commission (“Commission” or “FTC”).<sup>1</sup> I appreciate this opportunity to provide the Commission’s views on peer-to-peer file-sharing and protecting consumers online. This testimony, among other things, addresses the Commission’s law enforcement actions against fraud artists whose deceptive or unfair practices involve exposing consumers, including children,<sup>2</sup> to unwanted pornography on the Internet.<sup>3</sup> The testimony also recognizes that some peer-to-peer file sharing services, as opposed to other content providers that operate their own networks, may not provide sufficient opportunities for labeling or other controls that parents may find useful in protecting their children from objectionable content.

The Federal Trade Commission is the federal government's principal consumer protection agency. Congress has directed the Commission, under the FTC Act, to take law enforcement action against “unfair or deceptive acts or practices” in almost all sectors of the economy and to promote vigorous competition in the marketplace.<sup>4</sup> With the exception of certain industries and

---

<sup>1</sup>The written statement presents the views of the Federal Trade Commission. Oral statements and responses to questions reflect my views and not necessarily those of the Commission or any individual Commissioner.

<sup>2</sup>As the Committee is aware, the Commission also enforces the Children’s Online Privacy Protection Rule, which requires Web sites, primarily those directed to children, to obtain parental consent before collecting personal information from children under the age of 13. Our enforcement and education efforts under this Rule are not addressed in the testimony.

<sup>3</sup>The Commission has brought cases involving unfair or deceptive acts or practices related to the dissemination of online pornography to adults. *See, e.g., FTC v. Brian D. Westby* (FTC File No. 032 3030; Case No. 03 C 2540; ND IL; filed Apr. 15, 2003; released Apr. 17, 2003).

<sup>4</sup>15 U.S.C. § 45.

activities, the FTC Act provides the Commission with broad investigative and enforcement authority over entities engaged in, or whose business affects, commerce.<sup>5</sup> The FTC Act also authorizes the Commission to conduct studies and collect information, and, in the public interest, to publish reports on the information it obtains.<sup>6</sup>

Although the Internet has empowered consumers with instant access to a breadth of information about products and services that would have been unimaginable 20 years ago, fraud artists also have proven adept at exploiting this new technology for their own gain. They are the ultimate “early adopters” of new technology. And, they have seized on the Internet as a ready vehicle to find victims for their scams. In fact, the Commission’s consumer complaint data show that consumers increasingly report the Internet as the initial point of contact for fraud, and that the Internet has now outstripped the telephone as the source of first contact for fraud.

Many of these frauds are simply online variations of familiar, offline scams. To combat these new frauds, the FTC has brought over 300 Internet-related enforcement actions, including actions against alleged purveyors of online pornography. For example, the Commission sued John Zuccarini, who registered some 6,000 domain names that were misspellings of popular Web sites, for “mousetrapping” consumers.<sup>7</sup> In a ploy designed to capture teenaged and younger Internet users, Zuccarini registered 15 variations of the popular children's cartoon site,

---

<sup>5</sup>In addition to the FTC Act, the Commission also has responsibility under 46 additional statutes governing specific industries and practices.

<sup>6</sup>15 U.S.C. § 46(b) and (f). Section 46(f) of the FTC Act provides that “the Commission shall also have the power . . . to make public from time to time such portions of the information obtained by it hereunder as are in the public interest; and to make annual and special reports to Congress . . . .”

<sup>7</sup>*FTC v. John Zuccarini*, No. 01-CV-4854 (E.D. Pa. 2002).

www.cartoonnetwork.com, (e.g., “cartoon netwok” instead of “cartoon network”) and 41 variations on the name of teen pop star, Britney Spears. The Commission alleged in its complaint that surfers who looked for a site, but misspelled its Web address, were taken to the defendant's sites. Once consumers arrived, Zuccarini’s Web sites were programmed to take control of their Internet browsers and force the consumers to view explicit advertisements for pornographic Web sites, as well as Web sites advertising gambling and psychic services. The obstruction allegedly was so severe in this case that consumers often were forced to choose between taking up to twenty minutes to close out all of the Internet windows, or turning off their computers, and losing all of their “pre-mousetrap” work.

After being sued, Mr. Zuccarini disappeared. Fortunately, as a result of a cooperative working relationship between the FTC and the United States Attorney’s Office for the Southern District of New York, Mr. Zuccarini was arrested in a south Florida hotel room.<sup>8</sup> The U.S. Attorney’s Office issued an indictment charging Zuccarini with violations of the Truth in Domain Names Act.<sup>9</sup> He pled guilty to 49 counts of violating the Act and to one count concerning the possession of child pornography. In February 2004, the court sentenced Mr. Zuccarini to 30 months in prison. In addition, the Commission obtained a permanent injunction

---

<sup>8</sup>Benjamin Weiser, *Spelling It ‘Dinsey,’ Children on Web Got XXX*, N.Y. TIMES, Sept. 4, 2003, § B (Late Edition), at 1. At the time of his arrest, Mr. Zuccarini was surrounded by computer equipment and cash, all of which was seized by criminal authorities. A United States Postal Inspector served him with the Final Court Order in the Commission’s case.

<sup>9</sup>The Truth in Domain Names Act makes it unlawful to knowingly use a misleading domain name with the intent to attract a minor into viewing a visual depiction of sexually explicit conduct on the Internet. *See* 18 U.S.C. § 2252(B)(b). This Act is contained in the new “Amber Alert” law enacted in 2003.

barring Zuccarini from engaging in mousetrapping and imposing a \$1.8 million judgment.<sup>10</sup>

Similarly, unsolicited commercial email, or spam, is a nuisance, but it is also a ready source of fraud, including the fraudulent means to expose children to pornography. In a recent case against a spammer, the Commission alleged that the defendant sent email messages claiming that consumers had won a free Sony PlayStation 2 or other prize through a promotion purportedly sponsored by Yahoo, Inc., another ploy particularly attractive to children.<sup>11</sup> The Commission alleged that the Web site link contained in the email instead directed consumers first to a Web page that imitated the authentic Yahoo Web page. The imitation Yahoo Web site instructed consumers to download a program that supposedly would allow them to connect "toll-free" to a Web site where they could enter their name and address to claim their PlayStation 2. Consumers who followed the instructions were connected to a pornographic Web site through a 900-number, where they incurred charges of up to \$3.99 per minute. The Commission obtained orders barring the spammers from sending any email that misrepresents the identity of the sender or the subject of the email. The Commission also obtained a settlement with the company that created the modem software used by the spammers in this scheme which includes the requirement that it pay \$25,000 in alleged ill-gotten gains.<sup>12</sup>

---

<sup>10</sup>See [www.ftc.gov/opa/2002/05/cupcake.htm](http://www.ftc.gov/opa/2002/05/cupcake.htm).

<sup>11</sup>*FTC v. BTV Industries*, No. CV S-03-1306-LRH-RJJ (D. Nev. 2004).

<sup>12</sup>*Id.* The FTC's complaint against the software company, BTV Industries, and its principals, Rik Covell and Adam Lewis, alleges that the defendants violated the FTC's 900-Number Rule by failing to disclose clearly to consumers using their software that they would be connected to the Internet through a 900-number and would incur charges of up to \$3.99 per minute. The settlement permanently bars the defendants from failing to disclose the cost of accessing any 900-number pay-per-call service, as well as from misrepresenting that consumers have won a prize, that consumers will be connected to any Web site toll-free, and that any of BTV's products or services are associated with a third party.

As the name of the CAN-SPAM Act implies (Controlling the Assault of Non-Solicited Pornography and Marketing Act), addressing the abuses inflicted on the American public by purveyors of pornography was one of Congress' primary purposes in passing that legislation.

Section 5(d) of the CAN-SPAM Act<sup>13</sup> directed the Federal Trade Commission to adopt a rule requiring a mark or notice to be included in spam that contains sexually oriented material. The purpose of the notice is to inform recipients that a spam message contains sexually oriented material and to make it easier to filter out messages that recipients do not wish to receive.

The FTC's final rule prescribes the phrase "SEXUALLY-EXPLICIT:" as the mark or notice mandated by the CAN-SPAM Act<sup>14</sup> to be included in spam that includes either visual images or written descriptions of sexually explicit conduct.<sup>15</sup> The final rule follows the intention of the CAN-SPAM Act to protect email recipients from exposure to unwanted sexual images in spam, by requiring this mark to be included both in the subject line of any email message that contains sexually oriented material and in the electronic equivalent of a "brown paper wrapper" in the body of the message. This "brown paper wrapper" is what a recipient initially will see

---

<sup>13</sup>15 U.S.C. § 7704(d).

<sup>14</sup>The Commission published a notice of proposed rulemaking in the Federal Register on January 29, 2004, and accepted comments until February 17, 2004. The Commission received 89 comments, mostly from individual consumers applauding the Commission's proposal and expressing their concern about pornographic email to which they and their children were being subjected. The final rule also excludes sexually oriented materials from the subject line of a sexually explicit email message.

<sup>15</sup>CAN-SPAM defines "sexually explicit conduct" by reference to the Sexual Exploitation and Other Abuse of Children Act ("Abuse of Children Act"), 18 U.S.C. Section 2256, which in turn defines this phrase to mean "actual or simulated – (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person."

when opening a message containing sexually oriented material. The “brown paper wrapper” will include the prescribed mark or notice, certain other specified information, and no other information or images.

The Rule’s effective date is May 19, 2004, so starting then, senders of spam email that contains sexually oriented material must include the warning “SEXUALLY-EXPLICIT: ” in the subject line or face fines for violating the FTC Act or federal criminal law.<sup>16</sup>

As documented by reports from the General Accounting Office and the House Committee on Government Reform,<sup>17</sup> another distribution channel for pornographic content online is Peer-to-Peer (P2P) file-sharing software. P2P file-sharing software enables individual users to exchange files with other users. The FTC has engaged in educational efforts to assist consumers in protecting themselves from the risk of harm when they are downloading and using P2P file-sharing technology.

To warn consumers, including parents, about the risk that P2P software can pose, including the risk of exposure to online pornography, in July 2003, the FTC issued a consumer alert entitled, “File-Sharing: A Fair Share? Maybe Not.”<sup>18</sup> In this alert, the Commission warned consumers that P2P file-sharing software may be used to exchange pornography, as well as games, videos, and music that may be inappropriate for children. The FTC also alerted consumers to the security risks of improperly configuring P2P file-sharing software, including

---

<sup>16</sup>18 U.S.C. Section 2256. The Department of Justice enforces Section 2256.

<sup>17</sup>*See infra* note 27.

<sup>18</sup>*See* “File-Sharing: A Fair Share? Maybe Not,” at [www.ftc.gov/bcp/conline/pubs/alerts/shareart.htm](http://www.ftc.gov/bcp/conline/pubs/alerts/shareart.htm).

the risk that sensitive personal files inadvertently may be disclosed.<sup>19</sup>

The Commission also recently examined other implications of P2P file-sharing software at its workshop entitled “Monitoring Software on Your PC: Spyware, Adware, and Other Software” held on April 19, 2004.<sup>20</sup> This workshop was designed to provide us with information about the nature and extent of the problems related to spyware.<sup>21</sup>

The testimony at the workshop and the public comments received provide us with some insight concerning the relationship between P2P file-sharing technology and the distribution of spyware.<sup>22</sup> Workshop participants generally agreed that spyware often is bundled with free software applications, including P2P file-sharing software. In addition, participants noted that distributors of the free software – including the disseminators of P2P file-sharing applications – may not adequately disclose the bundling of spyware with the free software.

Some have suggested restricting the downloading of P2P file-sharing software

---

<sup>19</sup>In April 2004, the Commission likewise alerted businesses to the potential security risks of P2P file-sharing programs. The Council of Better Business Bureaus, with the cooperation of the Commission and the National Cyber Security Alliance, produced and widely distributed a brochure that provides a checklist of recommendations to help large and small businesses improve their computer security, and specifically alerts businesses to the possible risks associated with file-sharing programs.

<sup>20</sup>69 Fed. Reg. 8538 (Feb. 24, 2004), at [www.ftc.gov/os/2004/02/040217spywareworkshopfrn.pdf](http://www.ftc.gov/os/2004/02/040217spywareworkshopfrn.pdf).

<sup>21</sup>For the purposes of the workshop, the FTC staff tentatively described spyware as “software that aids in gathering information about a person or organization without their knowledge and which may send such information to another entity without the consumer’s consent, or asserts control over a computer without the consumer’s knowledge.” 69 Fed. Reg. 8538 (Feb. 24, 2004), at [www.ftc.gov/os/2004/02/040217spywareworkshopfrn.pdf](http://www.ftc.gov/os/2004/02/040217spywareworkshopfrn.pdf).

<sup>22</sup>The FTC received 200 comments about spyware by the time of the workshop, and public comment on this topic will be accepted until May 21, 2004. Public comments are posted on the FTC’s Web site at [www.ftc.gov/bcp/workshops/spyware/index.htm#comments](http://www.ftc.gov/bcp/workshops/spyware/index.htm#comments).



applications to combat the distribution of spyware. Participants at the workshop, however, emphasized that P2P file-sharing technology itself is neutral – but some participants argued that software applications may create harms for consumers. Accordingly, participants generally expressed the view that government and industry responses should focus on the spyware software that itself has adverse effects on consumers.

The Commission will continue to review the information from the workshop and related comments. Later this year, the FTC will issue a comprehensive report addressing spyware, including the relationship between P2P file-sharing software and spyware.

The FTC also has studied the effect of P2P file-sharing software in connection with its long-standing oversight of the marketing of violent entertainment to children. Since September 2000, the Commission has monitored the marketing of violent entertainment products to children by the motion picture, music recording, and electronic games industries. The FTC has issued four reports setting forth its findings.<sup>23</sup>

In connection with its ongoing review of these industries, the Commission staff recently examined four popular P2P file-sharing services to assess what online disclosures, if any, were made regarding the content of individual files shared by users of these services.<sup>24</sup> The four services examined offer consumers the ability to download free software that enables them to

---

<sup>23</sup>See, e.g., “Marketing Violent Entertainment to Children: A Review of Self-Regulation and Industry Practices in the Motion Picture, Music Recording & Electronic Game Industries” (Sept. 2000). To date, the Commission has issued three follow-up reports – in April and December of 2001, and in June of 2002.

<sup>24</sup>These file-sharing software services reviewed were Kazaa, Morpheus, LimeWire, and Overnet.

share files, including music downloads, with other users.<sup>25</sup> The files do not reside in a central location, but rather are stored on the hard drives of the users of the software. None of the P2P file-sharing services themselves label or otherwise provide notice about the content of any file. Instead, each user of a particular P2P file-sharing program places files in a shared folder on his or her own hard drive and thus can label or designate the file in any manner he or she chooses. Accordingly, each file, if labeled or otherwise described as having explicit content, would have been labeled by the individual user.

Each of the P2P file-sharing programs offered some type of filter to exclude unwanted content. Kazaa and LimeWire provided filters that blocked access to materials that contained offensive or otherwise adult-content related words in the description of the file. In addition, all four services gave users the ability to create their own filters by manually entering all the words that they wanted blocked from search results. All of these filters, however, operate by only examining language found in the title or descriptor of the file, rather than the content of the file.<sup>26</sup> Moreover, these filters may not be effective when users label files inaccurately, which can result in the transfer of files with pornographic or other unwanted content.<sup>27</sup>

---

<sup>25</sup>Such services may enable users to upload or download copyrighted recordings without first obtaining permission from the copyright holder.

<sup>26</sup>For example, music recordings that have been designated with a parental advisory by a recording company would be blocked by the filter only if a word in the title or descriptor of the file happened to be offensive. A recording company may have decided to apply the Parental Advisory Label to a particular recording for any number of reasons other than the presence of offensive words in the title.

<sup>27</sup>*See, e.g.*, “File-Sharing Programs: Peer-to-Peer Networks Provide Ready Access to Child Pornography,” General Accounting Office Report to the Chairman and Ranking Minority Member, Committee on Government Reform, U.S. House of Representatives (Feb. 2003); and “Children’s Access to Pornography Through Internet File-Sharing Programs,” prepared for Rep. Henry A. Waxman and Rep. Steve Largent by Minority Staff, Special Investigations Division,

## **Conclusion**

The FTC thanks the Subcommittee for this opportunity to describe how the Commission has used its authority under of Section 5 of the FTC Act to attack deceptive and unfair practices in the distribution of online pornography.

---

Committee on Government Reform, U.S. House of Representatives (July 27, 2001).